BAG15121 Discussion Draft S.L.C.
114TH CONGRESS
1ST SESSION

S. XXXX

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. BURR introduced the following bill; which was read twice and referred to the Committee on

A BILL

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Cybersecurity Information Sharing Act of 2015''.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

SEC. 2. DEFINITIONS.

In this Act:

(1) AGENCY.—The term ‘‘agency’’ has the meaning given the term in section 3502 of title 44, United States Code.

(2) ANTITRUST LAWS.—The term ‘‘antitrust laws’’—

(A) has the meaning given the term in section 1 of the Clayton Act (15 U.S.C. 12);

(B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and

(C) includes any State law that has the same intent and effect as the laws under sub-paragraphs (A) and (B).

(3) APPROPRIATE FEDERAL ENTITIES.—The term ‘‘appropriate Federal entities’’ means the following:

(A) The Department of Commerce.

(B) The Department of Defense.

(C) The Department of Energy.

(D) The Department of Homeland Security.

(E) The Department of Justice.

(F) The Department of the Treasury.

(G) The Office of the Director of National Intelligence.

(4~~5~~) CYBERSECURITY PURPOSE.—The term ‘‘cybersecurity purpose’’ means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

(5~~6~~) CYBERSECURITY THREAT.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term ‘‘cybersecurity threat’’ means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

(B) EXCLUSION.—The term ‘‘cybersecurity threat’’ does not include any action that —

~~(i)~~ solely involves a violation of a consumer term of service or a consumer licensing agreement~~; and~~

~~(ii) does not otherwise constitute unauthorized access~~.

(6~~7~~) CYBER THREAT INDICATOR.—The term ‘‘cyber threat indicator’’ means information that is necessary to describe or identify—
(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
(B) a method of defeating a security control or exploitation of a security vulnerability;
(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
(E) malicious cyber command and control;
(F) the actual or potential harm caused by an incident, including information exfiltrated when it is necessary in order to describe a cybersecurity threat;
(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
(H) any combination thereof.

(74) ~~COUNTERMEASURE~~DEFENSIVE MEASURE.—
(A) Except as provided in subparagraph (B), t~~T~~he term ‘‘defensive ~~counter~~measure’’ means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.
(B) EXCLUSION – The term “defensive measure” does not include a measure that destroys, renders unusable, or substantially harms an information system or data on an information system not belonging to-
(i) the private entity operating the measure; or
(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

(8) ENTITY.—
(A) IN GENERAL.—Except as otherwise provided in this paragraph, the term ‘‘entity’’ means any private entity, non-Federal government agency or department, or State, tribal, or local government (including a political subdivision, department, or component thereof).
(B) INCLUSIONS.—The term ‘‘entity’’ includes a government agency or department of the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands,

Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.
(C) Exclusion.—The term ''entity'' does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(9) Federal entity.—The term ''Federal entity'' means a department or agency of the United States or any component of such department or agency.

(10) Information system.—The term ''information system''—
(A) has the meaning given the term in section 3502 of title 44, United States Code; and
(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

(11) Local government.—The term ''local government'' means any borough, city, county, parish, town, township, village, or other political subdivision of a State.

(12) Malicious cyber command and control.—The term ''malicious cyber command and control'' means a method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

(13) Malicious reconnaissance.—The term ''malicious reconnaissance'' means a method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(14) Monitor.—The term ''monitor'' means to acquire, ~~obtain,~~ identify, or scan, or ~~otherwise~~ to possess information that is stored on, processed by, or transiting an information system.

(15) Private entity.—
(A) In general.—Except as otherwise provided in this paragraph, the term ''private entity'' means any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof.
(B) Inclusion.—The term ''private entity'' includes a State, tribal, or local

government performing electric utility services.
(C) EXCLUSION.—The term ''private entity'' does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).
(16) SECURITY CONTROL.—The term ''security control'' means the management, operational, and technical controls used to protect the confidentiality, integrity, and availability of an information system or its information.
(17) SECURITY VULNERABILITY.—The term ''security vulnerability'' means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.
(18) TRIBAL.—The term ''tribal'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

SEC. 3. SHARING OF INFORMATION BY THE FEDERAL GOVERNMENT.

(a) IN GENERAL.—Consistent with the protection of classified information, intelligence sources and methods, and ~~the protection of~~ privacy and civil liberties, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate Federal entities, shall develop and promulgate procedures to facilitate and promote—
(1) the timely sharing of classified cyber threat indicators in the possession of the Federal Government with cleared representatives of relevant entities;
(2) the timely sharing with relevant entities of cyber threat indicators or information in the possession of the Federal Government that may be declassified and shared at an unclassified level; and
(3) the sharing with relevant entities, or the public if appropriate, of unclassified, including controlled unclassified, cyber threat indicators in the possession of the Federal Government; and
(4) the sharing with entities, if appropriate, of information in the possession of the Federal Government about cybersecurity threats to such entities to prevent or mitigate adverse effects from such cybersecurity threats.~~.~~

(b) DEVELOPMENT OF PROCEDURES.—
(1) IN GENERAL.—The procedures developed and promulgated under subsection (a) shall—
(A) ensure the Federal Government has and maintains the capability to share cyber threat indicators in real time consistent with the protection of classified information;

(B) incorporate, to the greatest extent practicable, existing processes and existing roles and responsibilities of Federal and non-Federal entities for information sharing by the Federal Government, including sector specific information sharing and analysis centers; and

(C) include procedures for notifying entities that have received a cyber threat indicator from a Federal entity under this Act that is known or determined to be in error or in contravention of the requirements of this Act or another provision of Federal law or policy of such error or contravention.

(D) include requirements of Federal entities receiving cyber threat indicators or defensive measures to implement and utilize security controls to protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures; and

(E) include procedures that require a Federal entity, prior to the sharing of a cyber threat indicator—

(i) to review such cyber threat indicator to assess whether such cyber threat indicator contains any information that such Federal entity knows at the time of sharing to be personal information of or identifying a specific person not directly related to a cybersecurity threat and remove such information; or

(ii) to implement and utilize a technical capability configured to remove any personal information of or identifying a specific person not directly related to a cybersecurity threat.

(2) COORDINATION.—In developing the procedures required under this section, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General shall coordinate with appropriate Federal entities, including the National Laboratories (as defined in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801)), to ensure that effective protocols are implemented that will facilitate and promote the sharing of cyber threat indicators by the Federal Government in a timely manner.

(c) SUBMITTAL TO CONGRESS.—Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of the appropriate Federal entities, shall submit to Congress the procedures required by subsection (a).

SEC. 4. AUTHORIZATIONS FOR PREVENTING, DETECTING, ANALYZING, AND MITIGATING CYBERSECURITY THREATS.

(a) AUTHORIZATION FOR MONITORING.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, monitor—

(A) an information system of such private entity;
(B) an information system of another entity, upon written consent of such other entity;
(C) an information system of a Federal entity, upon written consent of an authorized representative of the Federal entity; and
(D) information that is stored on, processed by, or transiting an information system monitored by the private entity under this paragraph.
(2) CONSTRUCTION.—Nothing in this subsection shall be construed—
(A) to authorize the monitoring of an information system, or the use of any information obtained through such monitoring, other than as provided in this Act; or
(B) to limit otherwise lawful activity.

(b) AUTHORIZATION FOR OPERATION OF ~~COUNTERMEASURES~~ DEFENSIVE MEASURES.—
(1) IN GENERAL.—~~Except as provided in paragraph (2) and n~~Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, operate a ~~countermeasure~~ defensive measure that is applied to—
(A) an information system of such private entity in order to protect the rights or property of the private entity;
(B) an information system of another entity upon written consent of such entity for operation of such defensive ~~counter~~measure to protect the rights or property of such entity; and
(C) an information system of a Federal entity upon written consent of an authorized representative of such Federal entity for operation of such defensive ~~counter~~measure to protect the rights or property of the Federal Government.
~~(2) LIMITATION.—The authority provided in paragraph (1) does not include operation of any countermeasure that is designed or deployed in a manner that will intentionally destroy, disable, or substantially harm an information system not belonging to—~~
~~(A) the private entity operating such countermeasure; or~~
~~(B) another entity or Federal entity that has provided consent to that private entity for operation of such countermeasure in accordance with this subsection.~~
(2~~3~~) CONSTRUCTION.—Nothing in this subsection shall be construed—
(A) to authorize the use of a countermeasure other than as provided in this subsection; or
(B) to limit otherwise lawful activity.

(c) AUTHORIZATION FOR SHARING OR RECEIVING CYBER THREAT INDICATORS OR DEFENSIVE ~~COUNTER~~MEASURES.—
(1) IN GENERAL.—Except as provided in paragraph (2) and notwithstanding any

other provision of law, an entity may, for the purposes permitted under this Act and consistent with the protection of classified information, share with, or receive from, any other entity or the Federal Government a cyber threat indicator or defensive ~~counter~~measure.
(2) LAWFUL RESTRICTION.—An entity receiving a cyber threat indicator or defensive ~~counter~~measure from another entity or Federal entity shall comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicator or countermeasure by the sharing entity or Federal entity.
(3) CONSTRUCTION.—Nothing in this subsection shall be construed—
(A) to authorize the sharing or receiving of a cyber threat indicator or countermeasure other than as provided in this subsection; or
(B) to limit otherwise lawful activity.

(d) PROTECTION AND USE OF INFORMATION.—
(1) SECURITY OF INFORMATION.—An entity monitoring an information system, operating a defensive ~~counter~~measure, or providing or receiving a cyber threat indicator or defensive ~~counter~~measure under this section shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicator or defensive ~~counter~~measure.
(2) REMOVAL OF CERTAIN PERSONAL INFORMATION.—An entity sharing a cyber threat indicator pursuant to this Act shall, prior to such sharing—
(A) review such cyber threat indicator to assess whether such cyber threat indicator contains any information that the entity knows at the time of sharing to be personal information of or identifying a specific person not directly related to a cybersecurity threat and remove such information; or
(B) implement and utilize a technical capability configured to remove any information contained within such indicator that the entity knows at the time of sharing to be personal information of or identifying a specific person not directly related to a cybersecurity threat.
(3) USE OF CYBER THREAT INDICATORS AND DEFENSIVE ~~COUNTER~~MEASURES BY ENTITIES.—
(A) IN GENERAL.—Consistent with this Act, a cyber threat indicator or defensive ~~counter~~measure shared or received under this section may, for cybersecurity purposes—
(i) be used by an entity to monitor or operate a defensive ~~counter~~measure on—
(I) an information system of the entity; or
(II) an information system of another entity or a Federal entity upon the written consent of that other entity or that Federal entity; and
(ii) be otherwise used, retained, and further shared by an entity subject to—
(I) an otherwise lawful restriction placed by the sharing entity or Federal entity on

such cyber threat indicator or defensive ~~counter~~measure; or

(II) an otherwise applicable provision of law.

(B) CONSTRUCTION.—Nothing in this paragraph shall be construed to authorize the use of a cyber threat indicator or defensive ~~counter~~measure other than as provided in this section.

(4) USE OF CYBER THREAT INDICATORS BY STATE, TRIBAL, OR LOCAL GOVERNMENT.—

(A) LAW ENFORCEMENT USE.—

(i) PRIOR WRITTEN CONSENT.—Except as provided in clause (ii), a cyber threat indicator shared with a State, tribal, or local government under this section may, with the prior written consent of the entity sharing such indicator, be used by a State, tribal, or local government for the purpose of preventing, investigating, or prosecuting any of the offenses described in section 5(d)(5)(A)(vi).

(ii) ORAL CONSENT.—If exigent circumstances prevent obtaining written consent under clause (i), such consent may be provided orally with subsequent documentation of the consent.

(B) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator shared with a State, tribal, or local government under this section shall be—

(i) deemed voluntarily shared information; and

(ii) exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records.

(C) STATE, TRIBAL, AND LOCAL REGULATORY AUTHORITY.—

(i) ~~AUTHORIZATION~~IN GENERAL.—Except as provided in clause (ii), A cyber threat indicator or defensive measure shared with a State, tribal, or local government under this ~~section~~ Act shall not otherwise be directly used by any State, tribal, or local government to regulate, including an enforcement action, ~~a~~ the lawful activity of an entity, including an activity relating to monitoring, operating a defensive measure, or sharing of a cyber threat indicator.

(ii) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS. – A cyber threat indicator or defensive measures shared as described in clause (i) may, consistent with State, tribal, or local government regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of a regulation relating to such information systems.

~~(ii) LIMITATION.—A cyber threat indicator shared as described in clause (i)~~

(e) ANTITRUST EXEMPTION.—

(1) IN GENERAL.—Except as provided in section 8(e), it shall not be considered a violation of any provision of antitrust laws for 2 or more private entities to exchange or provide a cyber threat indicator, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity threat, for cybersecurity

purposes under this Act.
(2) APPLICABILITY.—Paragraph (1) shall apply only to information that is exchanged or assistance provided in order to assist with—
(A) facilitating the prevention, investigation, or mitigation of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system; or
(B) communicating or disclosing a cyber threat indicator to help prevent, investigate, or mitigate the effect of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system.

(f) NO RIGHT OR BENEFIT.—The sharing of a cyber threat indicator with an entity under this Act shall not create a right or benefit to similar information by such entity or any other entity.

SEC. 5. SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE ~~COUNTER~~MEASURES WITH THE FEDERAL GOVERNMENT.

(a) REQUIREMENT FOR POLICIES AND PROCEDURES.—
(1) INTERIM POLICIES AND PROCEDURES.—Not later than 60 days after the date of the enactment of this Act, the Attorney General, in coordination with the heads of the appropriate Federal entities, shall develop, and submit to Congress, interim policies and procedures relating to the receipt of cyber threat indicators and defensive ~~counter~~measures by the Federal Government.
(2) FINAL POLICIES AND PROCEDURES.—Not later than 180 days after the date of the enactment of this Act, the Attorney General shall, in coordination with the heads of the appropriate Federal entities, promulgate final policies and procedures relating to the receipt of cyber threat indicators and defensive ~~counter~~measures by the Federal Government.
(3) REQUIREMENTS CONCERNING POLICIES AND PROCEDURES.—Consistent with the guidelines developed under subsection (b), the policies and procedures developed and promulgated under this subsection shall—
(A) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 4(c) ~~that are received~~ through the real-time process described in subsection (c)—
(i) are shared in ~~real time~~an automated manner with ~~such receipt with~~ all of the appropriate Federal entities;
(ii) are not subject to any delay, modification, ~~interference,~~ or any other action that could impede real-time receipt by all of the appropriate Federal entities; and
(iii) may be provided to other Federal entities;
(B) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 4 in a manner other than the process described in

subsection (c) of this section—
(i) are shared ~~immediately~~ as quickly as operationally practicable with all of the appropriate Federal entities;
(ii) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities; and
(iii) may be provided to other Federal entities;
(C) consistent with this Act, any other applicable provisions of law, and the fair information practice principles set forth in appendix A of the document entitled ''National Strategy for Trusted Identities in Cyberspace'' and published by the President in April, 2011, govern the retention, use, and dissemination by the Federal Government of cyber threat indicators shared with the Federal Government under this Act, including the extent, if any, to which such cyber threat indicators may be used by the Federal Government; and
(D) ensure there is—
(i) an audit capability; and
(ii) appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under this Act in an unauthorized manner.
(4) GUIDELINES FOR ENTITIES SHARING CYBER THREAT INDICATORS WITH FEDERAL GOVERNMENT.—
(A) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Attorney General shall develop and make publicly available guidance to assist entities and promote sharing of cyber threat indicators with Federal entities under this Act.
(B) CONTENTS.—The guidelines developed and made publicly available under subparagraph (A) shall include guidance on the following:
(i) Identification of types of information that would qualify as a cyber threat indicator under this Act that would be unlikely to include personal information of or identifying a specific person not directly related to a cyber security threat.
(ii) Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat.
(iii) Such other matters as the Attorney General considers appropriate for entities sharing cyber threat indicators with Federal entities under this Act.

(b) PRIVACY AND CIVIL LIBERTIES.—
(1) GUIDELINES OF ATTORNEY GENERAL.—Not later than 60 days after the date of the enactment of this act, t~~T~~he Attorney General shall, in coordination with the heads of the appropriate Federal agencies and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1), develop, submit to Congress, and make available to the public

interim~~ and periodically review ~~ guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this Act.

(2) FINAL GUIDELINES.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1) and such private entities with industry expertise as the Attorney General considers relevant, promulgate final guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this Act.

(B) PERIODIC REVIEW.—The Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers and private entities described in subparagraph (A), periodically review the guidelines promulgated under subparagraph (A).

(3~~2~~) CONTENT.—The guidelines required by ~~ developed and reviewed under~~ paragraphs (1) and (2) shall, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats—

(A) limit the impact on privacy and civil liberties of activities by the Federal Government under this Act;

(B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of or identifying specific persons, including by establishing—

(i) a process for the timely destruction of information that is known not to be directly related to uses authorized under this Act; and

(ii) specific limitations on the length of any period in which a cyber threat indicator may be retained;

(C) include requirements to safeguard cyber threat indicators containing personal information of or identifying specific persons from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines;

(D) include procedures for notifying entities and Federal entities if information received pursuant to this section ~~that ~~is known or determined by a Federal entity receiving such information not to constitute a cyber threat indicator; ~~and~~

(E) protect the confidentiality of cyber threat indicators containing personal information of or identifying specific persons to the greatest extent practicable and require recipients to be informed that such indicators may only be used for purposes authorized under this Act; and

(F) include steps that may be needed so that dissemination of cyber threat indicators is consistent with the protection of classified and other sensitive national security information.~~.~~

(c) CAPABILITY AND PROCESS WITHIN THE DEPARTMENT OF HOMELAND SECURITY.—
(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the heads of the appropriate Federal entities, shall develop and implement a capability and process within the Department of Homeland Security that—
(A) shall accept from any entity in real time cyber threat indicators and defensive ~~counter~~measures, pursuant to this section;
(B) shall, upon submittal of the certification under paragraph (2) that such capability and process fully and effectively operates as described in such paragraph, be the process by which the Federal Government receives cyber threat indicators and defensive ~~counter~~measures under this Act that are shared by a private entity with the Federal Government through electronic mail or media, an interactive form on an Internet website, or a real time, automated process between information systems except—
(i) communications between a Federal entity and a private entity regarding a previously shared cyber threat indicator; and
~~(ii) voluntary or legally compelled participation in an open Federal investigation;~~
(ii~~i~~) communications by a regulated entity with such entity's Federal regulatory authority regarding a cybersecurity threat.~~; and~~
(iv) cyber threat indicators or countermeasures shared with a Federal entity as part of a contractual or statutory requirement;
(C) ensures that all of the appropriate Federal entities receive in an automated manner such cyber threat indicators ~~in real time with receipt~~ shared through the real-time process within the Department of Homeland Security;
(D) is in compliance with the policies, procedures, and guidelines required by this section; and
(E) does not limit or prohibit otherwise lawful disclosures of communications, records, or other information, including –
(i) reporting of known or suspected criminal activity, by an entity to any other entity or a Federal entity;
(ii) voluntary or legally compelled participation in a Federal investigation; and
(iii) providing cyber threat indicators or defensive measures as part of a statutory or authorized contractual requirement.~~.~~
(2) CERTIFICATION.—Not later than 10 days prior to the implementation of the capability and process required by paragraph (1), the Secretary of Homeland Security shall, in consultation with the heads of the appropriate Federal entities,

certify to Congress whether such capability and process fully and effectively operates—
(A) as the process by which the Federal Government receives from any entity a cyber threat indicator or defensive ~~counter~~measure under this Act; and
(B) in accordance with the policies, procedures, and guidelines developed under this section.
(3) PUBLIC NOTICE AND ACCESS.—The Secretary of Homeland Security shall ensure there is public notice of, and access to, the capability and process developed and implemented under paragraph (1) so that—
(A) any entity may share cyber threat indicators and defensive ~~counter~~measures through such process with the Federal Government; and
(B) all of the appropriate Federal entities receive such cyber threat indicators and defensive ~~counter~~measures in real time with receipt through the process within the Department of Homeland Security.
(4) OTHER FEDERAL ENTITIES.—The process developed and implemented under paragraph (1) shall ensure that other Federal entities receive in a timely manner any cyber threat indicators and defensive ~~counter~~measures shared with the Federal Government through such process.
(5) REPORT ON DEVELOPMENT AND IMPLEMENTATION.—
(A) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress a report on the development and implementation of the capability and process required by paragraph (1), including a description of such capability and process and the public notice of, and access to, such process.
(B) CLASSIFIED ANNEX.—The report required by subparagraph (A) shall be submitted in unclassified form, but may include a classified annex.

(d) INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.—
(1) NO WAIVER OF PRIVILEGE OR PROTECTION.—The provision of cyber threat indicators and defensive ~~counter~~measures to the Federal Government under this Act shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.
(2) PROPRIETARY INFORMATION.—Consistent with section 4(c)(2), a~~A~~ cyber threat indicator or defensive ~~counter~~measure provided by an entity to the Federal Government under this Act shall be considered the commercial, financial, and proprietary information of such entity when so designated by ~~such~~ the originating entity or a third party acting in accordance with the written authorization of the originating entity.
(3) EXEMPTION FROM DISCLOSURE.—Cyber threat indicators and defensive ~~counter~~measures provided to the Federal Government under this Act shall be—

(A) deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records; and
(B) withheld, without discretion, from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local provision of law requiring disclosure of information or records.
(4) EX PARTE COMMUNICATIONS.—The provision of a cyber threat indicator or defensive ~~counter~~measure to the Federal Government under this Act shall not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-~~-~~making official.
(5) DISCLOSURE, RETENTION, AND USE.—
(A) AUTHORIZED ACTIVITIES.—Cyber threat indicators and defensive ~~counter~~measures provided to the Federal Government under this Act may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—
(i) a cybersecurity purpose;
(ii) the purpose of identifying a cybersecurity threat, including the source of such cybersecurity threat, or a security vulnerability;
(iii) the purpose of identifying a cybersecurity threat involving the use of an information system by a foreign adversary or terrorist;
(iv~~ii~~) the purpose of responding to, or otherwise preventing or mitigating, an imminent threat of death or serious bodily harm, or serious economic harm, including~~;~~
~~(iv) the purpose of responding to, or otherwise preventing or mitigating,~~ a terrorist act or a ~~the development or~~ use of a weapon~~s~~ of mass destruction;
(v) the purpose of responding to, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or
(vi) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in clause (~~ii~~iv)~~, an offense arising out of an act, development or use described in clause (iv)~~, or any of the offenses listed in—
(I) section 3559(c)(2)(F) of title 18, United States Code (relating to serious violent felonies);
(II) sections 1028 through 1030 of such title (relating to fraud and identity theft);
(III) chapter 37 of such title (relating to espionage and censorship); and
(IV) chapter 90 of such title (relating to protection of trade secrets).
(B) PROHIBITED ACTIVITIES.—Cyber threat indicators and defensive ~~counter~~measures provided to the Federal Government under this Act shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under subparagraph (A).

(C) PRIVACY AND CIVIL LIBERTIES.— Cyber threat indicators and defensive ~~counter~~measures provided to the Federal Government under this Act shall be retained, used, and disseminated by the Federal Government—

(i) in accordance with the policies, procedures, and guidelines required by subsections (a) and (b);

(ii) in a manner that protects from unauthorized use or disclosure any cyber threat indicators that may contain personal information of or identifying specific persons; and

(iii) in a manner that protects the confidentiality of cyber threat indicators containing personal information of~~,~~ or ~~that~~ identifying~~ies,~~ a specific person.

(D) FEDERAL REGULATORY AUTHORITY.—

(i) IN GENERAL.—Except as provided in clause (ii), cyber threat indicators and defensive ~~counter~~measures provided to the Federal Government under this Act shall not be directly used by any Federal, State, tribal, or local government ~~department or agency~~ to regulate, including an enforcement action, the lawful activities of any entity, including activities relating to monitoring, operation of defensive ~~counter~~measures, or sharing of cyber threat indicators.

(ii) EXCEPTIONS.—

(I) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS.—Cyber threat indicators and defensive ~~counter~~measures provided to the Federal Government under this Act may, consistent with Federal or State regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such information systems.

(II) PROCEDURES DEVELOPED AND IMPLEMENTED UNDER THIS ACT.—Clause (i) shall not apply to procedures developed and implemented under this Act.

SEC. 6. PROTECTION FROM LIABILITY.

(a) MONITORING OF INFORMATION SYSTEMS.—No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of information systems and information under ~~subsection (a) of~~ section 4(a) that is conducted in accordance with this Act.

(b) SHARING OR RECEIPT OF CYBER THREAT INDICATORS.—No cause of action shall lie or be maintained in any court against any entity, and such action shall be promptly dismissed, for the sharing or receipt of cyber threat indicators or defensive ~~counter~~measures under section 4(c) if—

(1) such sharing or receipt is conducted in accordance with this Act; and

(2) in a case in which a cyber threat indicator or defensive ~~counter~~measure is shared with the Federal Government, the cyber threat indicator or defensive ~~counter~~measure is shared in a manner that is consistent with section 5(c)(1)(B) and the sharing or receipt, as the case may be, occurs after the earlier of—
(A) the date on which the interim policies and procedures are submitted to Congress under section 5(a)(1); or
(B) the date that is 60 days after the date of the enactment of this Act.

(c) CONSTRUCTION.—Nothing in this section shall be construed—
(1) to require dismissal of a cause of action against an entity that has engaged in gross negligence or willful misconduct in the course of conducting activities authorized by this Act; or
(2) to undermine or limit the availability of otherwise applicable common law or statutory defenses.

SEC. 7. OVERSIGHT OF GOVERNMENT ACTIVITIES.
(a) BIENNIAL REPORT ON IMPLEMENTATION.—
(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, and not less frequently than once every 2 years thereafter, the heads of the appropriate Federal entities shall jointly submit and the Inspector General of the Department of Homeland Security, the Inspector General of the Intelligence Community, the Inspector General of the Department of Justice, the Inspector General of the Department of Defense, and the Inspector General of the Department of Energy, in consultation with the Council of Inspectors General on Financial Oversight, shall jointly submit to Congress a detailed report concerning the implementation of this Act.
(2) CONTENTS.—Each report submitted under paragraph (1) shall include the following:
(A) An assessment of the sufficiency of the policies, procedures, and guidelines required by section 5 in ensuring that cyber threat indicators are shared effectively and responsibly within the Federal Government.
(B) An evaluation of the effectiveness of real-time information sharing through the capability and process developed under section 5(c), including any impediments to such real-time sharing.
(C) An assessment of the sufficiency of the procedures developed under section 3 in ensuring that cyber threat indicators in the possession of the Federal Government are shared in a timely and adequate manner with appropriate entities, or, if appropriate, are made publicly available.
(D) An assessment of whether cyber threat indicators have been properly classified and an accounting of the number of security clearances authorized by the Federal

Government for the purposes of this Act.
(E) A review of the type of cyber threat indicators shared with the Federal Government under this Act, including the following:
(i) The degree to which such information may impact the privacy and civil liberties of specific persons.
(ii) A quantitative and qualitative assessment of the impact of the sharing of such cyber threat indicators with the Federal Government on privacy and civil liberties of specific persons.
(iii) The adequacy of any steps taken by the Federal Government to reduce such impact.
(F) A review of actions taken by the Federal Government based on cyber threat indicators shared with the Federal Government under this Act, including the appropriateness of any subsequent use or dissemination of such cyber threat indicators by a Federal entity under section 5.
(G) A description of any significant violations of the requirements of this Act by the Federal Government.
(H) A ~~classified~~ summary of the number and type of entities that received classified cyber threat indicators from the Federal Government under this Act and an evaluation of the risks and benefits of sharing such cyber threat indicators.
(3) RECOMMENDATIONS.—Each report submitted under paragraph (1) may include ~~such~~ recommendations ~~as the heads of the appropriate Federal entities may have~~ for improvements or modifications to the authorities and processes under this Act.
(4) FORM OF REPORT.—Each report required by paragraph (1) shall be submitted in unclassified form, but ~~shall~~ may include a classified annex.

(b) REPORTS ON PRIVACY AND CIVIL LIBERTIES.—
(1) BIENNIAL REPORT FROM PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD.—Not later than 2 years after the date of the enactment of this Act and not less frequently than once every 2 years thereafter, the Privacy and Civil Liberties Oversight Board shall submit to Congress and the President a report providing—
(A) an assessment of the effect on privacy and civil liberties ~~impact of~~ by the type of activities carried out under this Act; and
(B) an assessment of the sufficiency of the policies, procedures, and guidelines established pursuant to section 5 in addressing privacy and civil liberties concerns.
(2) BIENNIAL REPORT OF INSPECTORS GENERAL.—
(A) IN GENERAL.—Not later than 2 years after the date of the enactment of this Act and not less frequently than once every 2 years thereafter, the Inspector General of the Department of Homeland Security, the Inspector General of the Intelligence Community, the Inspector General of the Department of Justice, the Inspector General of the Department of Defense, and the Inspector General of the

Department of Energy shall, in consultation with the Council of Inspectors General on Financial Oversight, jointly submit to Congress a report on the receipt, use, and dissemination of cyber threat indicators and defense ~~counter~~measures that have been shared with Federal entities under this Act.

(B) CONTENTS.—Each report submitted under subparagraph (A) shall include the following:

(i) A review of the types of cyber threat indicators shared with Federal entities.

(ii) A review of the actions taken by Federal entities as a result of the receipt of such cyber threat indicators.

(iii) A list of Federal entities receiving such cyber threat indicators.

(iv) A review of the sharing of such cyber threat indicators among Federal entities to identify inappropriate barriers to sharing information.

(3) RECOMMENDATIONS.—Each report submitted under this subsection may include such recommendations as the Privacy and Civil Liberties Oversight Board, with respect to a report submitted under paragraph (1), or the Inspectors General referred to in paragraph (2)(A), with respect to a report submitted under paragraph (2), may have for improvements or modifications to the authorities under this Act.

(4) FORM.—Each report required under this subsection shall be submitted in unclassified form, but may include a classified annex.

SEC. 8. CONSTRUCTION AND PREEMPTION.

(a) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this Act shall be construed--

(1) to limit or prohibit otherwise lawful disclosures of communications, records, or other information, including reporting of known or suspected criminal activity, by an entity to any other entity or the Federal Government under this Act; or

(2) to limit or prohibit otherwise lawful use of such disclosures by any Federal entity, even when such otherwise lawful disclosures duplicate or replicate disclosures made under this Act.~~.~~

(b) WHISTLE BLOWER PROTECTIONS.—Nothing in this Act shall be construed to prohibit or limit the disclosure of information protected under section 2302(b)(8) of title 5, United States Code (governing disclosures of illegality, waste, fraud, abuse, or public health or safety threats), section 7211 of title 5, United States Code (governing disclosures to Congress), section 1034 of title 10, United States Code (governing disclosure to Congress by members of the military), section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) (governing disclosure by employees of elements of the intelligence community), or any similar provision of Federal or State law.

(c) PROTECTION OF SOURCES AND METHODS.— Nothing in this Act shall be construed—
(1) as creating any immunity against, or otherwise affecting, any action brought by the Federal Government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, or use of classified information;
(2) to affect the conduct of authorized law enforcement or intelligence activities; or
(3) to modify the authority of a department or agency of the Federal Government to protect classified information and sources and methods and the national security of the United States.

(d) RELATIONSHIP TO OTHER LAWS.—Nothing in this Act shall be construed to affect any requirement under any other provision of law for an entity to provide information to the Federal Government.

(e) PROHIBITED CONDUCT.—Nothing in this Act shall be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.

(f) INFORMATION SHARING RELATIONSHIPS.—Nothing in this Act shall be construed—
(1) to limit or modify an existing information sharing relationship;
(2) to prohibit a new information sharing relationship;
(3) to require a new information sharing relationship between any entity and the Federal Government; or
(4) to require the use of the capability and process within the Department of Homeland Security developed under section 5(c).

(g) PRESERVATION OF CONTRACTUAL OBLIGATIONS AND RIGHTS.—Nothing in this Act shall be construed—
(1) to amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between any entities, or between any entity and a Federal entity; or
(2) to abrogate trade secret or intellectual property rights of any entity or Federal entity.

(h) ANTI-TASKING RESTRICTION.—Nothing in this Act shall be construed to permit the Federal Government—
(1) to require an entity to provide information to the Federal Government;

(2) to condition the sharing of cyber threat indicators with an entity on such entity's provision of cyber threat indicators to the Federal Government; or
(3) to condition the award of any Federal grant, contract, or purchase on the provision of a cyber threat indicator to a Federal entity.

(i) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this Act shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized in this Act.

(j) USE AND RETENTION OF INFORMATION.—Nothing in this Act shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal Government to retain or use any information shared under this Act for any use other than permitted in this Act.

(k) FEDERAL PREEMPTION.—
(1) IN GENERAL.—This Act supersedes any statute or other provision of law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this Act.
(2) STATE LAW ENFORCEMENT.—Nothing in this Act shall be construed to supersede any statute or other provision of law of a State or political subdivision of a State concerning the use of authorized law enforcement practices and procedures.

(l) REGULATORY AUTHORITY.—Nothing in this Act shall be construed—
(1) to authorize the promulgation of any regulations not specifically authorized by this Act;
(2) to establish or limit any regulatory authority not specifically established or limited under this Act; or
(3) to authorize regulatory actions that would duplicate or conflict with regulatory requirements, mandatory standards, or related processes under another provision of Federal law.

(m) AUTHORITY OF SECRETARY OF DEFENSE TO RESPOND TO CYBER ATTACKS.—Nothing in this Act shall be construed to limit the authority of the Secretary of Defense to develop, prepare, coordinate, or, when directed by the President to do so, conduct a military cyber operation in response to a cyber attack carried out against the United States or a United States person by a foreign government or an organization sponsored by a foreign government or a terrorist organization.

SEC. 9. REPORT ON CYBERSECURITY THREATS.

(a) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the heads of other appropriate elements of the intelligence community, shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on cybersecurity threats, including cyber attacks, theft, and data breaches.

(b) CONTENTS.—The report required by subsection (a) shall include the following:
(1) An assessment of the current intelligence sharing and cooperation relationships of the United States with other countries regarding cybersecurity threats, including cyber attacks, theft, and data breaches, directed against the United States and which threaten the United States national security interests and economy and intellectual property, specifically identifying the relative utility of such relationships, which elements of the intelligence community participate in such relationships, and whether and how such relationships could be improved.
(2) A list and an assessment of the countries and nonstate actors that are the primary threats of carrying out a cybersecurity threat, including a cyber attack, theft, or data breach, against the United States and which threaten the United States national security, economy, and intellectual property.
(3) A description of the extent to which the capabilities of the United States Government to respond to or prevent cybersecurity threats, including cyber attacks, theft, or data breaches, directed against the United States private sector are degraded by a delay in the prompt notification by private entities of such threats or cyber attacks, theft, and breaches.
(4) An assessment of additional technologies or capabilities that would enhance the ability of the United States to prevent and to respond to cybersecurity threats, including cyber attacks, theft, and data breaches.
(5) An assessment of any technologies or practices utilized by the private sector that could be rapidly fielded to assist the intelligence community in preventing and responding to cybersecurity threats.

(c) FORM OF REPORT.—The report required by subsection (a) shall be made available in classified and unclassified forms.

(d) INTELLIGENCE COMMUNITY DEFINED.—In this section, the term ''intelligence community'' has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

SEC. 10. CONFORMING AMENDMENTS.
(a) PUBLIC INFORMATION.—Section 552(b) of title 5, United States Code, is

amended—
(1) in paragraph (8), by striking ''or'' at the end;
(2) in paragraph (9), by striking ''wells.'' and inserting ''wells; or''; and
(3) by inserting after paragraph (9) the following:
''(10) information shared with or provided to the Federal Government pursuant to the Cybersecurity Information Sharing Act of 2015.''.

(b) MODIFICATION OF LIMITATION ON DISSEMINATION OF CERTAIN INFORMATION CONCERNING PENETRATIONS OF DEFENSE CONTRACTOR NETWORKS.—Section 941(c)(3) of the National Defense Authorization Act for Fiscal Year 2013 (Public Law 112–239; 10 U.S.C. 2224 note) is amended by inserting at the end the following:
''The Secretary may share such information with other Federal entities if such information consists of cyber threat indicators and defense ~~counter~~measures and such information is shared consistent with the policies and procedures promulgated by the Attorney General under section 5 of the Cybersecurity Information Sharing Act of 2015.''.